Datenschutz-Folgenabschätzung

Methode zur Vertrauensbildung

Martin Rost

Kiel, 31.08.2015

Gliederung

- Warum „Data-Protection-Impact-Assessment“ (DPIA) und nicht einfach „Privacy-Impact-Assessment“ (PIA)?
- Grundzüge des Standard-Datenschutzmodells (SDM) als Operationalisierung datenschutzrechtlicher Anforderungen
- Anforderungen an ein DPIA aus SDM-Sicht
- Diskussion von zwei PIA-Prozessframeworks

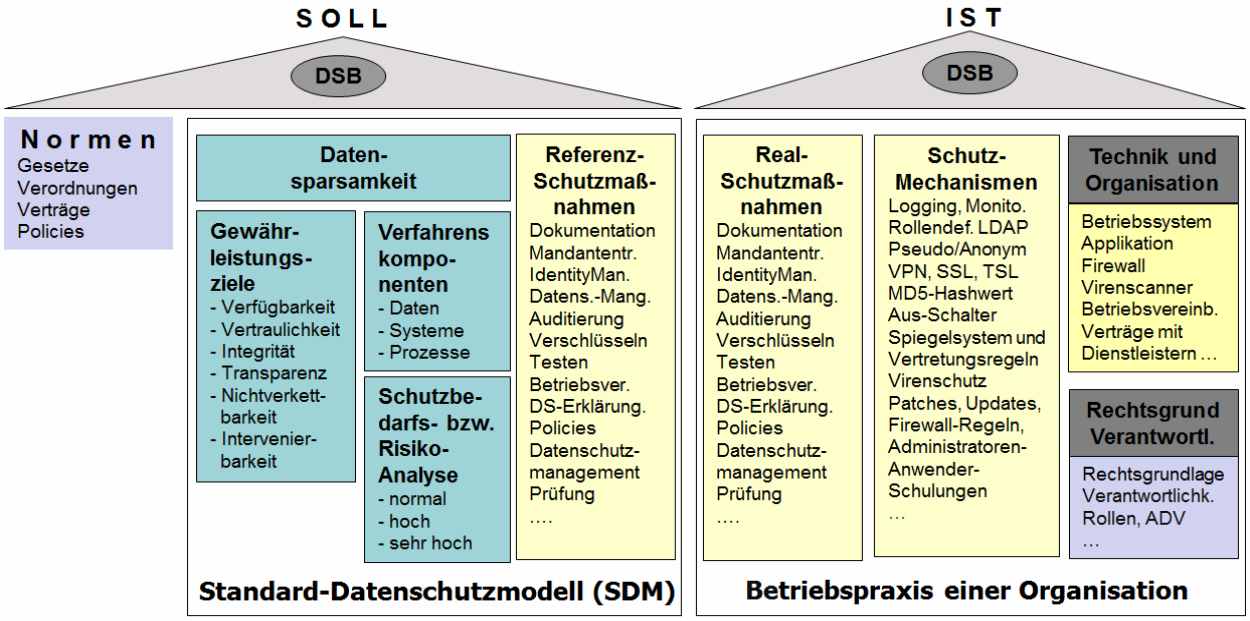
Warum Data-Protection-Impact-Assessment (DPIA)?

- Datenschutz thematisiert die **Machtasymmetrie** zwischen Organisationen (staatlichen Behörden, Unternehmen, Wissenschaftsinstituten) und deren „Personal“ (Bürger, Kunden, Patienten, Menschen, Individuen, MitarbeiterInnen).
- Aus Datenschutzsicht gilt **jede Organisation als ein Angreifer auf Personen**. Datenschutz setzt deshalb nicht bei einer „Idee von der Privatheit“ von Personen an, sondern bei den faktisch notorischen Angriffen von Organisationen auf Personen als strukturell schwächere Risikonehmer.
- **Privatheit kann entstehen, wenn mächtigere Organisationen Personen Autonomie abfordern!** Organisationen müssen dafür – mit ihrer automatisierten Datenverarbeitung, die notwendig Personen als Datenobjekte fasst – die Grundrechte achten.
- Ein DPIA zieht deshalb **Kriterien des Grundrechteschutz** (-> „elementare Schutzziele“) als relevante Risikodimensionen heran und formuliert typische Angriffsszenarien durch Organisationen.

Standard-Datenschutzmodell (SDM)

- Zweck des SDM: Vermittlung von grundrechtlichen Anforderungen sowie technischen und organisatorischen Funktionalitäten und Schutzmaßnahmen in Organisationen.
- SDM ...
  - basiert auf dem Konzept der „sechs elementaren Schutz-ziele“ (von DSB-Konferenz 2010 bestätigt);
  - differenziert die Verfahrenskomponenten Daten, IT-Systeme und Prozesse;
  - orientiert sich am Schutz von Personen, nicht am Schutz von Geschäftsprozessen;
  - unterscheidet Schutzbedarfe normal, hoch, sehr hoch;
  - orientiert sich methodisch am IT-Grundschutz des BSI.
- DSB-Konferenz bestätigte 2014 das SDM mit Auftrag, bis zum Herbst 2015 einen Referenzkatalog mit standardisierten Schutzmaßnahmen zu erstellen.

Standard-Datenschutzmodell



aus: „SDM-Handbuch“ der DSB-Konferenz, 2014.10, V0.8, S. 35

Wie bringt man nun ein (D)PIA und das SDM der deutschen Datenschutzaufsichtsbehörden zusammen?

PIA
Was gibt es?

- **Evaluation und Methodenüberblick**
  - Clarke: „An evaluation of privacy impact assessment guidance"
  - Wright et al.: Privacy Impact Assessment
- **ISO-Frameworks**
  - ISO 22307:2008 Financial services -- Privacy impact assessment
  - ISO 29100, Privacy Framework
  - ISO 29101, Privacy Reference Architecture
- **BSI / Spiekermann, Techfolg.-Abschätzung**
  - BSI: „Privacy Impact Assessment Guideline for RFID Applications" (2011)
  - Wright / Friedewald: „Integrating privacy and ethical impact assessments" (2013)
  - Oetzel / Spiekermann: „Privacy-By-Design through systematic privacy impact assessment – presentation of a methodology" (2013)
- **Standard-Datenschutzmodell (SDM)**
  - Rost / Bock: „Impact Assessment im Lichte des Standard-Datenschutzmodells" (2012/2015)
  - SDM der DSB-Konferenz / AK-Technik (2013)

Prozess-Framework, aber weder Operationalisierung von Grundrechten durch Kriterienkatalog noch Angreifernodell.

- Prozess-Framework,
- relevante Kriterien,
- Angreifermodell

Explikation
des Zwecks eines Impact Assessments

- **Marketing-PIA**
  Zweck: Aufsichtsbehörden und Kunden sollen ein PIA zum Nachweis des Erfüllens datenschutzrechtlicher Anforderungen akzeptieren. Typische Form: Extrem schmaler Target-of-Evaluation; Prüfkriterien intransparent oder Kriterien der IT-Sicherheit werden mit denen des Datenschutzrechts gleichgesetzt; Methodik: formal korrekt durchgeführtes ISO-Verfahren, mit rechtlich ungeklärter Relevanz. Negative Folgen für Bürger, Kunden, Patienten zu ermitteln, wird von vornherein vermieden oder Ergebnisse nicht veröffentlicht.
- **Data-Protection-Impact-Assessment**
  Zweck: Nachweis der Konformität mit datenschutzrechtlichen Anforderungen. DPIA kann dazu dienen, die grundrechtlich geforderten Schutzmaßnahmen für ein Objekt in einem personenbezogenen Verfahren ausfindig zu machen. Sinnvoll: Rückgriff auf das Standard-Datenschutzmodell.
- **Wissenschaftliche Technikfolgen-Abschätzung**
  Zweck: *Aufdecken unbekannter Eigenschaften und Risiken*, ist objektiv bzw. ergebnisoffen angelegt, darf spekulativ sein, offene Methodik, Evaluation auch verschiedener Methoden sinnvoll; Publikation auch negativer Ergebnisse.

Katalog relevanter Angreifermotive für ein DPIA

Untersuchungsfrage: Inwieweit unterstützt das Prüfobjekt typische Angreifermotive (der anwendenden Organisation)? Legt das Prüfobjekt eine Überdehnung des Zwecks nahe?

- Staatliche Sicherheitsbehörden
  - Innenministerien, Polizei, Geheimdienste, Militärs, Verwaltung
- Staatliche Leistungsverwaltung
  - Hartz IV, Rente
- Unternehmen
  - Hersteller des Prüfobjekts
  - Banken, Versicherung
  - Adresshändler und Scoring/Profilierungs-Unternehmen
  - IT-Provider (Access, Content, Services)
  - Krankenhäuser
- Forschungseinrichtungen (Medizin- und Sozialforschung, Psychologie)
- Interessensvereinigung, Arbeitgeber

relevanter Komponenten eines DPIAs

Die für ein zu prüfendes Objekt auszuweisenden relevanten Komponenten:

- *Daten:* Welche (neuen?) personenbezogenen Daten lassen sich mit dem Prüfobjekt erzeugen?
- *IT-System:* Welche (neuen) Formen einer automatisierten Datenverarbeitung sind mit dem neuen Prüfobjekt möglich?
- *Prozesse:* Welche neue Qualität entsteht im Kontext der strukturellen Angreifer-Interessen? Welche Verwertungsprozesse in der Zwecknachbarschaft sind denkbar?

Schutzperspektive und Schutzbedarfe eines DPIAs

Untersuchung des Prüfobjekts im Hinblick darauf, welcher **Schutzbedarf** (normal, hoch, sehr hoch) durch die Nutzung des Prüfobjekts durch organisierte Angreifer aus der **Schutzperspektive** einer Einzelpersonenrolle (eines Bürgers, Kunden, Patienten, Menschen, Individuums, Subjekts) entsteht.

Katalog der Risikokriterien eines DPIAs

- Als Risikokriterien sind die sechs elementaren Schutzziele des Datenschutzes heranzuziehen, die an Grundrechten, nicht an „monetären Schäden für den Einzelnen“, gekoppelt sind. Zu den sechs elementaren Schutzzielen zählen:
  - Verfügbarkeit
  - Integrität
  - Vertraulichkeit
  - Transparenz
  - Nicht-Verkettbarkeit
  - Intervenierbarkeit
- Die Risiken lassen sich ausweisen durch
  - eine Negation von Schutzzielen (Intransparenz, Verkettung...)
  - eine Bestimmung strukturell gegebener Angreifermotive (nicht durch individualisierte Schadensszenarien einzelner Betroffener)

Schutzziele Warum?

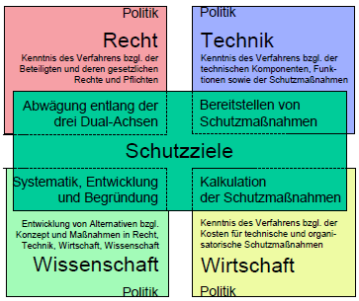
1. Schutzziele decken Anforderungen aus dem BDSG (u.a. Anhang zu §9) vollständig ab.

Tabelle: Zuordnung der gesetzlichen Vorgaben zu den Gewährleistungszielen.

Datensparsamkeit	Verfügbarkeit	Integrität	Vertraulichkeit	Nichtverkettbarkeit	Transparenz	Intervenierbarkeit
	Nr. 7 der Anlage zu § 9	Nr. 1 6 der Anlage zu § 9	Nr. 1 6 sowie Satz 2 der Anlage zu § 9	Nr. 8 der Anlage zu § 9		
§ 3a				§ 4 Abs. 3 Nr. 2	§ 4 Abs. 3	§ 4 Abs. 1
§ 4 Abs. 2 Nr. 2a				§ 4a Abs. 1 Satz 2	§ 4a Abs. 1 Satz 2 4, Abs. 2 Satz 2, Abs. 3	§ 4c Abs. 1 Satz 1 Nr. 1
§ 6 b Abs. 3, 5				§ 4b Abs. 6	§ 4d Abs. 1 Satz 1, § 4d Abs. 5	§ 6 Abs. 1, § 6 Abs. 2 Satz 1

„SDM-Handbuch“ der DSB-Konferenz, 2014.10, V0.8, S. 15

2. Schutzziele vermitteln jeweils zwischen Recht/Politik, Wirtschaft, Wissenschaft und der Technik.



Rost: Zur Konditionierung von Recht und Technik, Gesellschaft für Inform. 2013

3. Integritäts- und Vertraulichkeitsurteil des BVerfG 2008/02.

Katalog an Referenz-Maßnahmen

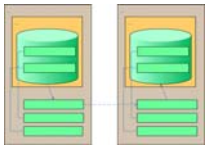
Zu jedem Schutziel gibt es einen Katalog an Maßnahmen mit unterschiedlichen Graden an Wirkintensität. Welche Wirkintensität angemessen ist, wird vom Schutzbedarf eines Verfahrens bzw. der im Verfahren erhobenen, gespeicherten, verarbeiteten Daten gesteuert.

Maßnahmen zur Sicherung der Verfügbarkeit

Verfügbarkeit:
Informationen sind dort und dann zugänglich,
wo und wann sie von Berechtigten gebraucht werden.

Schutz von Verfügbarkeit: Gewährleisten von Funktionalität gegen vorsätzliche oder versehentliche Einschränkung, z.B. durch

- **Redundanz** (Daten, Hardware)
- Wartung
- Backup



www.openclipart.org

Maßnahmen zur Sicherung der Integrität

Integrität: Informationen sind richtig, vollständig und aktuell oder aber dies ist erkennbar nicht der Fall.

Schutz von Integrität:
Verhindern von unberechtigter Manipulation oder Datenverlust, z.B. durch

- Prüfsummen, fehlerkorrigierende Codes
- Einschränkung von Schreibrechten
- Definition von Soll/Ist-Zuständen und deren Überprüfung bei Prozessen
- Erkennen von Manipulationen durch Zeitstempel
- **Signaturen und Prüfsummen**

www.openclipart.org

Maßnahmen zur Sicherung der Vertraulichkeit

Vertraulichkeit:
Informationen dürfen nur Berechtigten bekannt werden.

Schutz von Vertraulichkeit:
Verhindern von unberechtigter Kenntnisnahme,
z.B. durch

- **Verschlüsselung** von Daten (Kryptographie)
- Verstecken von Daten (Steganographie)
- **Zugriffsbeschränkungen** durch Authentisierung- und Autorisierung (Rollenkonzept)

```
-----BEGIN PGP-----
0IxWZHhKYoECwCBeIweKU+0Ed
m068SB4ADeGGCtd+eacjDT5Ig
TdwAypl8+WOFYxTVEXbqOqjoW
mY4T9zuoSC5e
=lu9g
-----END PGP-----
```


Maßnahmen zur Sicherung der Transparenz

Transparenz: Ein Verfahren erfüllt prüfbar die datenschutzrechtlich bestehenden Anforderungen.

Sicherung von Transparenz:

- **Dokumentation** von Verfahren, d.h. der Datenbestände, der IT-Systeme sowie der technischen Funktionen und organisatorischen Regelungen
- **Protokollierung** der Prozesse

Maßnahmen zur Sicherung der Nicht-Verkettbarkeit

Nicht-Verkettbarkeit: Ein personenbezogenes Verfahren darf nur für den bestimmten Zweck verwendet werden.

Sicherung von Nicht-Verkettbarkeit:

- Zweck für Verfahren (und einzelne Bestandteile) festlegen, von anderen (verwandten) Zwecken trennen und technisch-organisatorisch binden
- Rollenkonzept: Autorisierung für Initiierung- / Lesen- / Schreiben- / Lösch-Aktivitäten
- **Trennung von Verfahren** durch Trennung der Datenbestände, IT-Systeme (Hardware/ Software) und Prozesse

www.openclipart.org

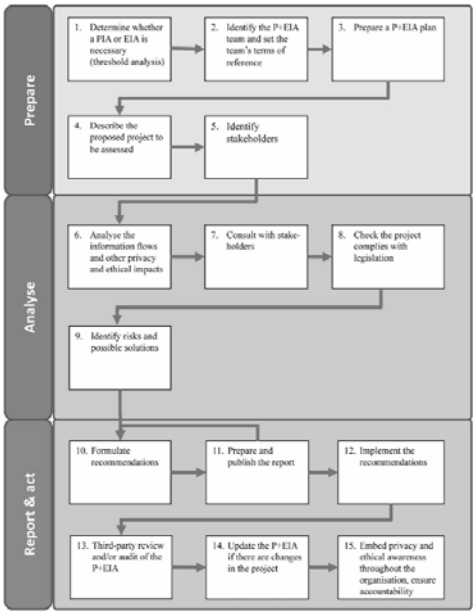
Maßnahmen zur Sicherung der Intervenierbarkeit

Intervenierbarkeit: Ein personenbezogenes Verfahren muss verändert werden können.

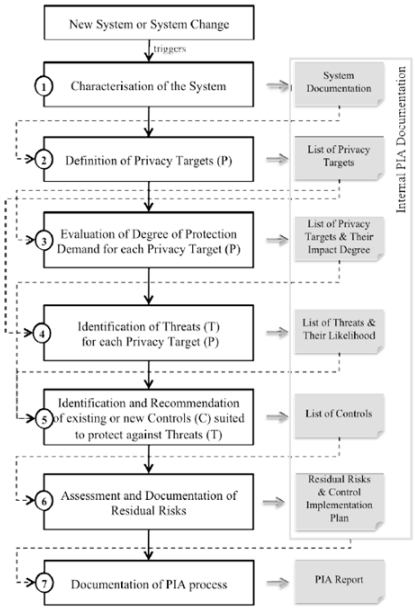
Sicherung von Intervenierbarkeit:

- Nutzen eines reifen **Changemanagements** für
  - Störungen
  - Problembearbeitungen
  - strukturelle Änderungen einer Organisation
- Single-Point-of-Contact für Betroffene, Verfahrensverfolgung

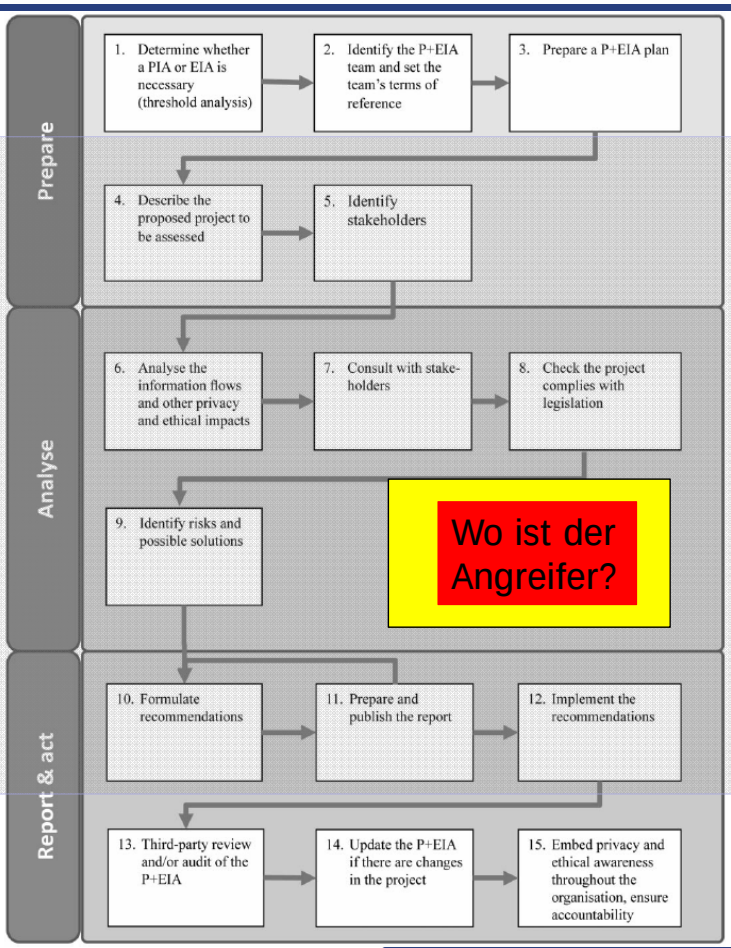
Zwei aktuelle wissenschaftliche PIA-Frameworks



Wright / Friedewald 2013: 763



Oetzel / Spiekermann 2013: 11

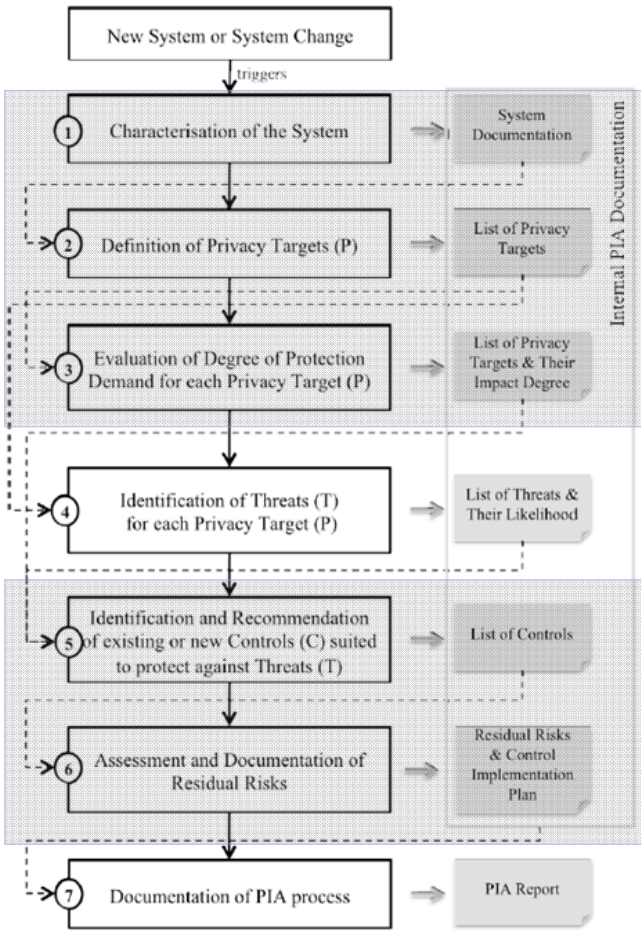


PIA (Wright/Friedewald 2013)

- Verfahrensbeschreibung einschl. verantwortliche Stelle, Prüfplanung
- Identifikation von Daten und Datenflüssen, Rechtsgrundlagen
- Schutzziele und Schutzmaßnahmen
- Sicherheitskonzept und Umsetzung — SDM
- Review des PIA und Fortschreibung

(Wright / Friedewald 2013: 763)

PIA+SDM=DPIA



← Verfahrensbeschreibung (inkl. Rechtsgrundlagen)

← DS-Recht/Schutzziele

← Schutzbedarf

SDM

← Katalog struktureller Angreifermotive

DPIA-spezifisch

← Katalog der Schutzmaßnahmen

← Sicherheitskonzept

SDM

(Oetzel / Spiekermann 2013: 11)

Besondere materielle Herausforderungen für ein (D)PIA

Personenbeziehbarkeit von Daten ist immer gegeben weil vom Kontext abhängig: „Es gibt kein belangloses Datum.“ (BVerfG 1983)

Eine Pseudonymisierung oder Anonymisierung von Daten schützt nicht vor einer Typisierung personenbezogener Daten. Eine Typisierung ermöglicht Organisationen, eine Risiko-Diskriminierung von Mitgliedern in Teilgruppen vorzunehmen. Diese Diskriminierung muss nicht auf Einzelperson heruntergerechnet werden und sie muss nicht „stimmen“, nicht „wahr“ oder „integer“ oder „valide und reliabel“, sondern nur relativ besser als die der Konkurrenz sein.

Schutzbedarf ist auch kontextabhängig: Besteht kein rechtsstaatlicher Schutz (keine Gesetze, keinen Vollzug), dann erhöht das den unmittelbaren Schutzbedarf von Personen gegenüber Organisationen.

Beispiele für erste Ansätze eines DPIA

Risikodiskussion anhand der Schutzziele und Angreifermodellierungen:

- ULD 2011: “Juristische Fragen im Bereich Altersgerechter Assistenzsysteme”, ULD, Technical Report, https://www.datenschutzzentrum.de/projekte/aal/

- Zwingelberg, H.; Hansen, M, 2012: “Privacy Protection Goals and Their Implications for eID Systems,” in Privacy and Identity Management for Life, ser. IFIP Advances in Information and Communication Technology, J. Camenisch et. al. vol. 375. Springer, 2012, pp. 245–260.

- DSK 2012: Orientierungshilfe “Datenschutzgerechtes Smart-Metering” https://www.datenschutz-bayern.de/technik/orient/oh_smartmeter.pdf

- Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, 01037/12/EN, Article 29 Data Protection Working Party Std. WP 196, Adopted July 1st 2012

Literaturhinweise zu PIA

- AK-Technik, 2013: Handreichung *„Anforderungen an Privacy Impact Assessments aus Sicht der Datenschutzaufsichtsbehörden“*
https://www.datenschutz-mv.de/datenschutz/publikationen/informat/pia/pia.pdf
- BSI, 2011: “Privacy Impact Assessment Guideline for RFID Applications”
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf;jsessionid=4BE04C3871C6AEB0CD78E76F22F0153A.2_cid244?__blob=publicationFile
- Clarke, R,, 2011: An evaluation of privacy impact assessment guidance documents; in: International Data Privacy Law, 2011: Vol. 1, No. 2, S. 111-120.
http://www.rogerclarke.com/DV/PIAG-Eval.html
- **Oetzel, M.; Spiekermann S., 2013: “*Privacy-By-Design through systematic privacy impact assessment – presentation of a methodology”*, European Journal of Information Systems (EJIS), July Vol. 23: 126-150**
- **Rost, M.; Bock, K., 2012: „*Impact Assessment im Lichte des Standard-Datenschutzmodells“*; in: Datenschutz und Datensicherheit, (DuD), 36. Jahrgang, Heft 10: 472-477.**
- Wright, D.; De Hert, P. (ed.), 2012: *Privacy Impact Assessment*, Dordrecht Heidelberg London New York, Springer.
- Wright, D.; Friedewald, M., 2013: Integrating privacy and ethical impact assessments; in: Science and Public Policy, Nr. 40: 755-766
- Wright, D.; Friedewald, M.; Gellert, R., 2015: Developing and testing a surveillance impact assessment methodogy; in: International Data Privay Law, Vol 5, No. 1: 40-53

Vielen Dank für Ihre Aufmerksamkeit

Martin Rost
ULD32@datenschutzzentrum.de
0431 9881391
Holstenstraße 98, 24103 Kiel